

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-289324

(43)Date of publication of application : 19.10.1999

(51)Int.Cl.

H04L 9/08  
G06F 12/14  
G06F 19/00  
G06K 17/00  
G06K 19/10  
G09C 1/00

(21)Application number : 10-091169

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 03.04.1998

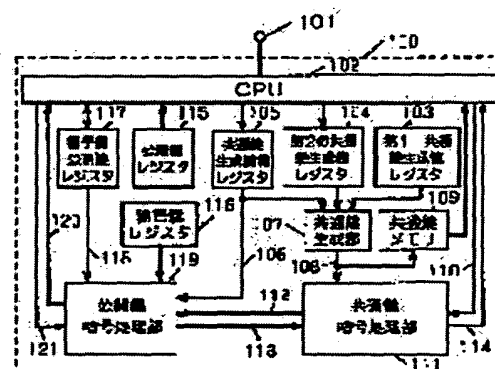
(72)Inventor : KASHIWA HIROSHI

## (54) TRANSMITTER-RECEIVER AND TRANSMISSION-RECEPTION METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance the confidentiality of an IC card and IC card system, using an enciphering method of a common key, a public key and a secret key.

SOLUTION: A public key register 115 is transferred to another party, an another party public key register 117 on the transmission side and the public key register 115 on the reception side are stored in the second common key generation register, a common key 108 is generated from the first common key generation value register 103 and the second common key generation value register 104 on the basis of common key generation information 106, the common key generation information 106 is transferred to the other party, and a common key whose value is shared by the other party is generated. It becomes possible to improve the confidentiality of an IC card 100 and an IC card system using the IC card 100, by making the common key 108 a key of a common key ciphering system and performing enciphering through combining it with the public key ciphering system.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-289324

(43) 公開日 平成11年(1999)10月19日

| (51) Int.Cl. <sup>8</sup>            | 識別記号  | F I           |         |  |
|--------------------------------------|-------|---------------|---------|--|
| H 0 4 L 9/08                         |       | H 0 4 L 9/00  | 6 0 1 C |  |
| G 0 6 F 12/14                        | 3 2 0 | G 0 6 F 12/14 | 3 2 0 B |  |
|                                      | 19/00 | G 0 6 K 17/00 | T       |  |
| G 0 6 K 17/00                        |       |               | E       |  |
|                                      |       | G 0 9 C 1/00  | 6 6 0 G |  |
| 審査請求 未請求 請求項の数10 O L (全 10 頁) 最終頁に続く |       |               |         |  |

(21) 出願番号 特願平10-91169

(22) 出願日 平成10年(1998)4月3日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 柏 浩

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

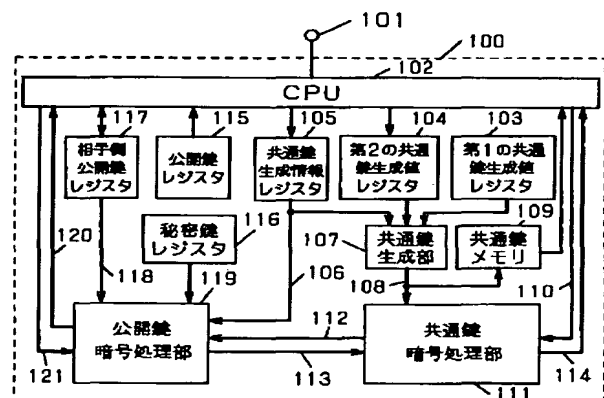
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 送受信装置および送受信方法

## (57) 【要約】

【課題】 共通鍵、公開鍵、秘密鍵を用いた暗号方法を用いたICカードおよびICカードシステムの機密性を高めることを目的とする。

【解決手段】 公開鍵レジスタ115を相手側に転送し、送信側なら相手側公開鍵レジスタ117、受信側なら公開鍵レジスタ115を第2の共通鍵生成レジスタに格納し、共通鍵生成情報106をもとに第1の共通鍵生成値レジスタ103と第2の共通鍵生成値レジスタ104から共通鍵108を生成し、相手側に共通鍵生成情報106を転送し、相手側も同じ値を有する共通鍵を生成する。共通鍵108を共通鍵暗号方式の鍵とし、公開鍵暗号方式と組み合わせて暗号を行うことにより、ICカード100およびICカード100を用いたICカードシステムの機密性を高めることが可能となる。



## 【特許請求の範囲】

【請求項 1】共通鍵を生成するための共通鍵生成値と、共通鍵を生成するための生成方法を示す共通鍵生成情報を受信し、前記共通鍵生成情報をもとに前記共通鍵生成値から共通鍵を生成し、前記受信した共通鍵生成値および共通鍵生成情報を送信することを特徴とする送受信装置。

【請求項 2】共通鍵を生成するための第 1 の共通鍵生成値を有し、共通鍵を生成するための第 2 の共通鍵生成値と、共通鍵を生成するための生成方法を示す共通鍵生成情報を受信し、前記共通鍵生成情報をもとに前記第 1 および第 2 の共通鍵生成値から共通鍵を生成し、前記受信した第 2 の共通鍵生成値および共通鍵生成情報を送信することを特徴とする送受信装置。

【請求項 3】請求項 1 および 2 記載の送受信装置において、受信した共通鍵生成情報を、第 2 の共通鍵生成情報に更新し、前記第 2 の共通鍵生成情報を送信する機能を有することを特徴とする送受信装置。

【請求項 4】請求項 3 記載の送受信装置において、第 2 の共通鍵生成情報を、定められた時間内において異なる値にする機能を有することを特徴とする送受信装置。

【請求項 5】公開鍵を更新する機能を有することを特徴とする送受信装置。

【請求項 6】請求項 5 記載の送受信装置において、公開鍵を更新した後に、前記更新した公開鍵を秘密鍵と入れ替えることを特徴とする送受信装置。

【請求項 7】共通鍵に関する情報を少なくとも 1 回公開鍵により暗号化する機能と、公開鍵を少なくとも 1 回共通鍵により暗号化する機能を有することを特徴とする送受信装置。

【請求項 8】第 1 の送受信装置は、第 2 の送受信装置に第 1 の公開鍵を送信し、第 2 の送受信装置は共通鍵を生成するための第 1 の共通鍵生成情報を生成し、前記第 1 の共通鍵生成情報をもとに前記受信した第 1 の公開鍵と第 1 の共通鍵生成値から第 1 の共通鍵を生成し、前記受信した第 1 の公開鍵を鍵として前記第 1 の共通鍵生成情報を暗号化して第 1 の暗号化データを生成し、前記第 1 の共通鍵を鍵として第 2 の公開鍵を暗号化して第 2 の暗号化データを生成し、前記第 2 の暗号データを前記受信した第 1 の公開鍵で暗号化して第 3 の暗号データを生成し、前記第 1 および第 3 の暗号データを前記第 1 の送受信装置に転送し、前記第 1 の送受信装置は前記第 1 の公開鍵に対応した秘密鍵を鍵として前記第 1 の暗号化データを復号化して第 1 の復号化データを生成し、前記第 1 の復号化データを鍵として前記第 1 の公開鍵と前記第 1 の共通鍵生成値と同じ値を有する第 2 の共通鍵生成値から前記第 1 の共通鍵と同じ値を有する第 2 の共通鍵を生成し、前記秘密鍵を鍵として前記転送された第 3 の暗号化データを復号化して第 2 の復号化データを生成し、前記第 2 の共通鍵を鍵として前記第 2 の復号化データを復

号化して前記第 2 の公開鍵と等しい第 3 の公開鍵を生成する機能を有することを特徴とする送受信方法。

【請求項 9】第 1 の送受信装置は共通鍵を生成するための第 1 の共通鍵生成情報を生成し、前記第 1 の共通鍵情報をもとに第 1 および第 2 の共通鍵生成値から第 1 の共通鍵を生成し、前記第 1 の共通鍵生成情報を第 2 の送受信装置に送信し、第 2 の送受信装置は前記受信した第 1 の共通鍵生成情報をもとに前記第 1 および第 2 の共通鍵生成値とそれぞれ同じ値を有する第 3 および第 4 の共通鍵生成値から前記第 1 の共通鍵と同じ値を有する第 2 の共通鍵を生成し、前記第 2 の送受信装置は第 2 の共通鍵生成情報を生成し、前記第 2 の共通鍵生成情報をもとに前記第 3 および第 4 の共通鍵生成値から第 3 の共通鍵を生成して前記第 2 の共通鍵に上書きし、前記第 2 の共通鍵生成情報を前記第 1 の送受信装置に送信し、前記第 1 の送受信装置は、前記受信した第 2 の共通鍵生成情報をもとに前記第 1 および第 2 の共通鍵生成値から前記第 3 の共通鍵と同じ値を有する第 4 の共通鍵を生成し、前記第 1 の共通鍵に上書きする機能を有することを特徴とする送受信方法。

【請求項 10】請求項 8 および 9 記載の送受信方法において、第 1 の送受信装置は、第 1 の認証データを暗号化して第 1 の暗号化データを生成し、前記第 1 の暗号化データを第 2 の送受信装置に送信し、前記第 2 の送受信装置は、前記受信した第 1 の暗号化データを復号化して第 1 の復号化データを生成し、前記第 1 の復号化データと前記第 1 の認証データと同じ値を有する第 2 の認証データの値が等しいならば第 1 の認証が成立したとし、第 3 の認証データを暗号化して第 2 の暗号化データを生成し、前記第 2 の暗号化データを前記第 1 の送受信装置に送信し、前記第 1 の送受信装置は前記受信した第 2 の暗号化データを復号化して第 2 の復号化データを生成し、前記第 2 の復号化データと前記第 3 の認証データと同じ値を有する第 4 の認証データの値が等しいならば第 2 の認証が成立したとし、前記第 1 および第 2 の認証が成立することをもって相互認証を行う機能を有することを特徴とする送受信方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、共通鍵、公開鍵、秘密鍵からなる暗号を用いた送受信装置および送受信方法に関するものである。

【0002】

【従来の技術】図 6 は、従来の共通鍵暗号方式と公開鍵暗号方式を用いた送受信装置における、送信側 IC カードの内部ブロック図を示す。なお、受信側 IC カードの内部構造は送信側 IC カードと同じである。

【0003】図 6 において、IC カード 600 は、送受信を行う相手側 IC カードとのデータの入出力を行う入出力端子 601 を備える。CPU 602 は、IC カード

600の内部を制御する。乱数発生部603は、相手ICカードに転送する乱数を発生し、乱数をCPU602に転送する。相手側乱数レジスタ604は相手側ICカードから送られてきた乱数を格納する。共通鍵レジスタ605は、共通鍵暗号方式における共通鍵を格納する。共通鍵は、送信側と受信側ICカードで同じ値を有する。共通鍵暗号処理部606は、共通鍵暗号方式により、共通鍵605に格納した共通鍵を鍵として、相手側乱数レジスタ604に格納した相手側乱数を暗号化しデータ607を生成し、また、データ608を復号化してデータ609を生成する。公開鍵レジスタ610は、公開鍵暗号方式に用いる公開鍵を格納する。秘密鍵レジスタ611は、公開鍵暗号方式に用いる秘密鍵を格納する。相手側公開鍵レジスタ612は、相手側ICカードから転送された相手側ICカードの公開鍵を格納する。公開鍵暗号処理部613は、公開鍵暗号方式により、相手側公開鍵レジスタ612に格納した相手側公開鍵を鍵としてデータ607を暗号化してデータ614を生成し、また、相手側ICカードから転送されてきたデータ615を復号化してデータ608を生成する。

【0004】次に、従来の公開鍵暗号方式と共通鍵暗号方式を用いた暗号方法による、送信側ICカードと受信側ICカードの間の相互認証動作を図7に示す。なお、CKEとCKDは各々、共通鍵暗号処理部606で行う共通鍵暗号方式による暗号化と復号化、PKEとPKDは各々、公開鍵暗号処理部613で行う公開鍵暗号方式による暗号化と復号化を表わす。

【0005】図7において、送信側ICカード700と受信側ICカード701の相互認証の方法を、STEP71～STEP74のステップで示す。ここで、データ送信側ICカード700は、公開鍵Dと、秘密鍵Dと、乱数Dと、共通鍵を有する。また、データ受信側ICカード701は、公開鍵Eと、秘密鍵Eと、乱数Eと、公開鍵を有する。また、送信側ICカード700と受信側のICカード701の内部構造は同じであり、送信側と受信側を入れ換えても以下に説明する動作と同様の動作を行う。以下、ステップ毎に説明を行う。

【0006】STEP71：送信側ICカード700は、乱数Dと公開鍵Dを受信側ICカード701に転送する。

【0007】STEP72：受信側ICカード701は、乱数Dを共通鍵暗号方式により共通鍵を鍵として暗号化してデータSD0を生成し、データSD0を公開鍵暗号方式により公開鍵Dを鍵として暗号化してデータSD1生成する。そして、データSD1と公開鍵Eと乱数Eを送信側ICカード700に転送する。

【0008】STEP73：送信側ICカード700は、データSD1を公開鍵暗号方式により秘密鍵Dを鍵として復号化してデータSD2を生成し、データSD2を共通鍵暗号方式により共通鍵を鍵として復号化してデ

ータSD3を生成する。そして、SD3と乱数Dを比較して、両者が一致した場合には受信側ICカード701を認証し、一致しない場合には認証エラーとする。認証が成立した場合には、乱数Eを共通鍵暗号方式により共通鍵を鍵として暗号化してデータSD4を生成し、データSD4を公開鍵暗号方式により公開鍵Eを鍵として暗号化してデータSD5を生成する。そうして、データSD5を受信側ICカード701に転送する。

【0009】STEP74：受信側ICカード701

10 は、データSD5を公開鍵暗号方式により秘密鍵Eを鍵として復号化してデータSD6を生成し、データSD6を共通鍵暗号方式により、共通鍵を鍵として復号化し、データSD7を生成する。そして、SD7と乱数Eを比較して両者が一致した場合は送信側ICカード700を  
15 認証して相互認証は完了する。一致しない場合には認証エラーとする。

【0010】

【発明が解決しようとする課題】しかしながら、上記の従来の共通鍵と公開鍵と秘密鍵を用いた送受信装置および送受信方法では、共通鍵と公開鍵と秘密鍵が固定されているため、一度それらが公知になると、次回からそれらの鍵を用いた暗号方法による送信側ICカードと受信側ICカードのデータ転送が意味をなさなくなり、ICカードおよびICカードシステムの機密性が低いという  
25 課題を有していた。

【0011】

【課題を解決するための手段】上記課題を解決するために、請求項1に記載の発明にかかる送受信装置は、共通鍵を生成するための共通鍵生成値と、共通鍵を生成するための生成方法を示す共通鍵生成情報を受信し、前記共通鍵生成情報をもとに前記共通鍵生成値から共通鍵を生成し、前記受信した共通鍵生成値および共通鍵生成情報を送信するものである。

【0012】上記構成により、送受信装置間で転送する共通鍵の生成情報だけでは共通鍵の内容を知る事はできないので、その共通鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

【0013】上記課題を解決するために、請求項2に記載の発明にかかる送受信装置は、共通鍵を生成するための第1の共通鍵生成値を有し、共通鍵を生成するための第2の共通鍵生成値と、共通鍵を生成するための生成方法を示す共通鍵生成情報を受信し、前記共通鍵生成情報をもとに前記第1および第2の共通鍵生成値から共通鍵を生成し、前記受信した第2の共通鍵生成値および共通鍵生成情報を送信するものである。

【0014】上記構成により、共通鍵の組み合わせの数を増加させることができるので、その共通鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

50 【0015】上記課題を解決するために、請求項3に記

載の発明にかかる送受信装置は、請求項 1 および 2 記載の送受信装置において、受信した共通鍵生成情報を、第 2 の共通鍵生成情報に更新し、前記第 2 の共通鍵生成情報を送信する機能を有するものである。

【0016】上記構成により、請求項 1、2 記載の発明の効果に加え、共通鍵の組み合わせの数をさらに増加させることができるので、その共通鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

【0017】上記課題を解決するために、請求項 4 に記載の発明にかかる送受信装置は、請求項 3 記載の送受信装置において、第 2 の共通鍵生成情報を、定められた時間内において異なる値にするものである。

【0018】上記構成により、請求項 3 記載の発明の効果に加えて、定められた時間内において同じ共通鍵が使われることがないので、その共通鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

【0019】上記課題を解決するために、請求項 5 に記載の発明にかかる送受信装置は、公開鍵を更新する機能を有するものである。

【0020】上記構成により、公開鍵が 1 つの値に固定されることがないので、その公開鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

【0021】上記課題を解決するために、請求項 6 に記載の発明にかかる送受信装置は、請求項 5 記載の送受信装置において、公開鍵を更新した後に、前記更新した公開鍵を秘密鍵と入れ替えるものである。

【0022】上記構成により、請求項 5 記載の発明の効果に加え、公開鍵と秘密鍵が 1 つの値に固定されることがないので、上記公開鍵と秘密鍵を用いた送受信装置において、その送受信における機密性を高めることが可能となる。

【0023】上記課題を解決するために、請求項 7 に記載の発明にかかる送受信装置は、共通鍵に関する情報を少なくとも 1 回公開鍵により暗号化する機能と、公開鍵を少なくとも 1 回共通鍵により暗号化する機能を有するものである。

【0024】上記構成により、共通鍵と公開鍵の機密性を高めることができるので、それらの鍵を用いた送受信装置において、送受信の機密性を高めることが可能となる。

【0025】上記課題を解決するために、請求項 8 に記載の発明にかかる送受信方法は、第 1 の送受信装置は、第 2 の送受信装置に第 1 の公開鍵を送信し、第 2 の送受信装置は共通鍵を生成するための第 1 の共通鍵生成情報を生成し、前記第 1 の共通鍵生成情報をもとに前記受信した第 1 の公開鍵と第 1 の共通鍵生成値から第 1 の共通鍵を生成し、前記受信した第 1 の公開鍵を鍵として前記第 1 の共通鍵生成情報を暗号化して第 1 の暗号化データを生成し、前記第 1 の共通鍵を鍵として第 2 の公開鍵を暗号化して第 2 の暗号化データを生成し、前記第 2 の暗

号データを前記受信した第 1 の公開鍵で暗号化して第 3 の暗号データを生成し、前記第 1 および第 3 の暗号データを前記第 1 の送受信装置に転送し、前記第 1 の送受信装置は前記第 1 の公開鍵に対応した秘密鍵を鍵として前記第 1 の暗号化データを復号化して第 1 の復号化データを生成し、前記第 1 の復号化データを鍵として前記第 1 の公開鍵と前記第 1 の共通鍵生成値と同じ値を有する第 2 の共通鍵生成値から前記第 1 の共通鍵と同じ値を有する第 2 の共通鍵を生成し、前記秘密鍵を鍵として前記転送された第 3 の暗号化データを復号化して第 2 の復号化データを生成し、前記第 2 の共通鍵を鍵として前記第 2 の復号化データを復号化して前記第 2 の公開鍵と等しい第 3 の公開鍵を生成する機能を有するものである。

【0026】上記構成により、公開鍵の機密性を高めることができるので、その公開鍵を用いた送受信方法を用いることにより、送受信の機密性を高めることが可能となる。

【0027】上記課題を解決するために、請求項 9 に記載の発明にかかる送受信方法は、第 1 の送受信装置は共通鍵を生成するための第 1 の共通鍵生成情報を生成し、前記第 1 の共通鍵情報をもとに第 1 および第 2 の共通鍵生成値から第 1 の共通鍵を生成し、前記第 1 の共通鍵生成情報を第 2 の送受信装置に送信し、第 2 の送受信装置は前記受信した第 1 の共通鍵生成情報をもとに前記第 1 および第 2 の共通鍵生成値とそれぞれ同じ値を有する第 3 および第 4 の共通鍵生成値から前記第 1 の共通鍵と同じ値を有する第 2 の共通鍵を生成し、前記第 2 の送受信装置は第 2 の共通鍵生成情報を生成し、前記第 2 の共通鍵生成情報をもとに前記第 3 および第 4 の共通鍵生成値から第 3 の共通鍵を生成して前記第 2 の共通鍵に上書きし、前記第 2 の共通鍵生成情報を前記第 1 の送受信装置に送信し、前記第 1 の送受信装置は、前記受信した第 2 の共通鍵生成情報をもとに前記第 1 および第 2 の共通鍵生成値から前記第 3 の共通鍵と同じ値を有する第 4 の共通鍵を生成し、前記第 1 の共通鍵に上書きする機能を有するものである。

【0028】上記構成により、共通鍵の機密性を高めることが可能となるので、それを用いた送受信方法を用いることにより、送受信の機密性を高めることが可能となる。

【0029】上記課題を解決するために、請求項 10 に記載の発明にかかる送受信方法は、請求項 8 および 9 記載の送受信方法において、第 1 の送受信装置は、第 1 の認証データを暗号化して第 1 の暗号化データを生成し、前記第 1 の暗号化データを第 2 の送受信装置に送信し、前記第 2 の送受信装置は、前記受信した第 1 の暗号化データを復号化して第 1 の復号化データを生成し、前記第 1 の復号化データと前記第 1 の認証データと同じ値を有する第 2 の認証データの値が等しいならば第 1 の認証が成立したとし、第 3 の認証データを暗号化して第 2

の暗号化データを生成し、前記第 2 の暗号化データを前記第 1 の送受信装置に送信し、前記第 1 の送受信装置は前記受信した第 2 の暗号化データを復号化して第 2 の復号化データを生成し、前記第 2 の復号化データと前記第 3 の認証データと同じ値を有する第 4 の認証データの値が等しいならば第 2 の認証が成立したとし、前記第 1 および第 2 の認証が成立することをもって相互認証を行う機能を有するものである。

【0030】上記構成により、請求項 8 および 9 に記載の発明の効果をを用いることにより、相互認証に用いるデータの機密性を高めることができるので、その認証方法を用いた送受信方法を用いることにより、送受信の機密性を高めることが可能となる。

【0031】

【発明の実施の形態】以下、本発明に係わる実施の形態について、図面を参照しながら説明する。

【0032】（実施の形態 1）図 1 は、本発明の実施の形態 1 に係るブロック図である。図 1 において、IC カード 100 は、送受信を行う相手側 IC カードとのデータの入出力を行う入出力端子 101 を備えている。CPU 102 は、IC カード 100 の内部を制御する。第 1 の共通鍵生成値レジスタ 103 には、共通鍵を生成するために必要な 2 つのデータのうちの 1 つ目のデータを格納する。第 2 の共通鍵生成値レジスタ 104 には、共通鍵を生成するために必要な 2 つのデータのうちの 2 つ目のデータを格納する。共通鍵生成情報レジスタ 105 は、第 1、第 2 の共通鍵生成値レジスタの値からどのように共通鍵を生成するかを示すデータである共通鍵生成情報 106 を格納する。共通鍵生成部 107 は、第 1 の共通鍵生成値レジスタ 103 と第 2 の共通鍵生成値レジスタ 104 と共通鍵生成情報 106 から共通鍵 108 を生成する。共通鍵メモリ 109 は、過去の定められた期間の共通鍵を格納し、CPU 102 はその期間内において同じ共通鍵が生成されないように、生成する共通鍵生成情報を管理する。共通鍵暗号処理部 111 は共通鍵暗号方式により、共通鍵 108 を鍵としてデータ 110 を暗号化してデータ 112 を生成し、また、データ 113 を復号化してデータ 114 を生成する。公開鍵レジスタ 115 は公開鍵暗号方式に用いる公開鍵を格納する。秘密鍵レジスタ 116 は公開鍵暗号方式に用いる秘密鍵を格納する。相手側公開鍵レジスタ 117 は、相手側 IC カードから転送された相手側の公開鍵を格納する。公開鍵処理部 119 は、公開鍵暗号方式により、相手側公開鍵 118 を鍵にして共通鍵生成情報 106 やデータ 112 を暗号化してデータ 120 を生成し、また、データ 121 を復号化してデータ 113 を生成する。

【0033】図 2 に、共通鍵生成部 107 の内部ブロック図を示す。第 1 のビット入れ換え回路 200 は共通鍵生成情報 106 により第 1 の共通鍵生成用レジスタ 103 のビットを入れ換えて第 1 のデータ 201 を生成す

る。同様に、第 2 のビット入れ換え回路 202 は、共通鍵生成情報 106 により第 2 の共通鍵生成用レジスタ 104 のビットを入れ換えて第 2 のデータ 203 を生成する。排他的論理和生成回路 204 は、第 1 のデータ 201 と第 2 のデータ 203 をビット毎に排他的論理和を生成し、共通鍵 108 を生成する。

【0034】図 3 に、本発明の第 1 の実施の形態に係わる相互認証の手順を示す。ここで、ある回の相互認証において、送信側 IC カード 300 は公開鍵 A と、秘密鍵 A と、第 1 の共通鍵生成値と、第 2 の共通鍵生成値として相手側公開鍵レジスタ 117 の値、すなわち相手側の公開鍵である公開鍵 B とを有し、共通鍵生成情報として共通鍵生成情報 A を生成するとする。また、その相互認証において受信側 IC カード 301 は、公開鍵 B と、秘密鍵 B と、第 1 の共通鍵生成値と、第 2 の共通鍵生成値として公開鍵 B、共通鍵生成情報として共通鍵生成情報 B を生成するものとする。以上の設定のもと、相互認証の手順を STEP 31～STEP 35 にそって説明する。なお、CKE と CKD は各々、共通鍵暗号処理部 111 で行う共通鍵暗号方式による暗号化と復号化、PKE と PKD は各々、公開鍵暗号処理部 119 で行う公開鍵暗号方式による暗号化と復号化、CKM は共通鍵生成部 107 で行う共通鍵生成処理を表わす。

【0035】STEP 31：受信側 IC カード 301 は、公開鍵 B を送信側 IC カード 300 に転送する。

【0036】STEP 32：送信側 IC カード 300 は、共通鍵生成情報 A により第 1 の共通鍵生成値と公開鍵 B から共通鍵 A を生成する。また、共通鍵生成情報 A を、公開鍵暗号方式により公開鍵 B を鍵として暗号化してデータ TD0 を生成する。また、公開鍵 A を、共通鍵暗号方式により共通鍵 A を鍵として暗号化してデータ TD1 を生成し、データ TD1 を公開鍵暗号方式により公開鍵 B を鍵として暗号化してデータ TD2 を生成する。そして、データ TD0 とデータ TD2 を受信側 IC カード 301 に転送する。

【0037】STEP 33：受信側 IC カード 301 は、データ TD0 を公開鍵暗号方式により秘密鍵 B を鍵として復号化し、共通鍵生成情報 A を生成する。そして、共通鍵生成情報 A により第 1 の共通鍵生成値と公開鍵 B より共通鍵 A を生成する。また、データ TD2 を公開鍵暗号方式により秘密鍵 B を鍵として復号化してデータ TD3 を生成し、データ TD3 を共通鍵暗号方式により共通鍵 A を鍵として復号化して公開鍵 A を生成する。そして、共通鍵生成情報 A を共通鍵生成情報 B に更新し、共通鍵生成情報 B により第 1 の共通鍵生成値と公開鍵 B から共通鍵 B を生成する。また、共通鍵生成情報 B を公開鍵暗号方式により、公開鍵 A を鍵として暗号化してデータ TD5 を生成する。また、データ TD3 を共通鍵暗号方式により共通鍵 B を鍵として暗号化してデータ TD6 を生成し、データ TD6 を公開鍵暗号方式により

公開鍵Aを鍵として暗号化してデータTD7を生成する。そして、データTD5とデータTD7を送信側ICカード301に転送する。

【0038】STEP34：送信側ICカード300は、データTD5を共通鍵暗号方式により秘密鍵Aを鍵として復合化して共通鍵生成情報Bを生成し、それまで保持していた共通鍵生成情報Aを共通鍵生成情報Bに更新する。そして、共通鍵生成情報Bにより第1の共通鍵生成値と公開鍵Bから共通鍵Bを生成する。また、データTD7を公開鍵暗号方式により秘密鍵Aを鍵として復号化してデータTD8を生成し、データTD8を共通鍵暗号方式により共通鍵Bを鍵として復号化してデータTD9を生成する。そして、データTD9とデータTD1の値を比較して両者が一致すれば受信側ICカード301を認証する。一致しないときは認証エラーとする。そして、一致した時は、データTD8を共通鍵暗号方式により共通鍵Bを鍵として暗号化してデータTD10を生成し、データTD10を共通鍵暗号方式により共通鍵Bを鍵として暗号化してデータTD11を生成する。そして、データTD11を受信側ICカード301に転送する。

【0039】STEP35：受信側ICカード301は、データTD11を公開鍵暗号方式により秘密鍵Bを鍵として復号化してデータTD12を生成し、データTD12を共通鍵暗号方式により共通鍵Bを鍵として復号化してデータTD13を生成する。そして、データTD13とデータTD6を比較して両者が一致すれば送信側ICカード300を認証する。

【0040】以上の構成により、次の1、2の理由によりICカードの共通鍵、公開鍵、秘密鍵の機密性が高まるので、それらの鍵を用いた暗号方法を用いることにより、ICカードおよびICカードシステムの機密性を高めることが可能となる。

【0041】1. 共通鍵や公開鍵や秘密鍵が公知になる可能性が低くなる。共通鍵はICカードの内部で生成され、また、相手側ICカードに同じ共通鍵を所有させるために、共通鍵そのものを転送するのではなく、共通鍵を生成させるための情報を転送し、相手側ICカード内部でも同様に共通鍵を生成させるため、ICカードの内部構造がわかなくとも共通鍵は導けないので、共通鍵が公知になる可能性は低くなる。

【0042】また、送信側ICカードの公開鍵をこの共通鍵を鍵として暗号化されて転送するので、公開鍵が公知になる可能性が低くなる。公開鍵が公知になる可能性が低くなるので、暗号化復号化関係にある秘密鍵が公知になる可能性も低くなる。

【0043】2. 共通鍵が公知になっても、共通鍵は更新される。共通鍵が公知になっても、共通鍵は相互認証における最初の認証までは鍵として用いられる度に更新されるので、公知となった共通鍵を用いて次の共通鍵暗

号方式の暗号化復号化を行うことはできない。

【0044】また、ICカードは共通鍵の履歴を格納するメモリを有しており、その履歴の期間内は同じ値の共通鍵は使わないようにするために、公知になった共通鍵をすぐに繰り返し使ってしまうことがなく、それによってさらに機密性は高くなる。

【0045】なお、以上の説明では、共通鍵生成部は、ビット入れ換え回路と排他論理和生成回路で構成したが、ビット演算ができれば、排他的論理和生成回路でなくとも、論理和回路や論理積回路などが行える回路であればよい。また、ビット演算でなくとも、ある規則に則って2つのデータから1つのデータが可逆的に演算できれば、どのような演算であってもよい。

【0046】なお、以上の説明では、共通鍵を生成するために2つの共通鍵生成値を用いる構成で説明したが、共通鍵生成値を1つにして、1つの共通鍵生成値のビット操作およびビット演算を行って共通鍵の生成を行う構成も同様に実施可能である。

【0047】なお、共通鍵生成情報は、共通鍵を使う度に更新してもよい。

(実施の形態2) 実施の形態2は、実施の形態1で説明した動作に加えて、公開鍵と秘密鍵を更新することを可能にした発明の一実施の形態を示すものである。

【0048】図4(a)に本発明の実施の形態2に係わるICカード400と公開鍵秘密鍵更新装置401との公開鍵秘密鍵を更新する時の接続の図を示す。ICカード400は、本実施の形態のICカードの本体である。公開鍵秘密鍵更新装置401は、ICカード400の公開鍵と秘密鍵を更新する装置である。暗号データの転送には共通鍵暗号方式が用いられる。

【0049】図4(b)に、ICカード400のブロック図を示す。同図において、符号101~114、117~121で示したものは、実施の形態1として図1に示した同符号の部分に対応する。特別コード402は、ICカード400が公開鍵秘密鍵更新装置401を認証するのに用いられ、公ICカード400が開鍵秘密鍵更新装置401も特別コードを有する事が確認できた事をもって認証が成立する。また、共通鍵には第1の共通鍵生成値レジスタ104の値を用いる。そのため、第2の共通鍵生成レジスタ103のデータは0にリセットし、また、共通鍵生成情報105には第1の共通鍵生成値レジスタのビットがそのまま出力される信号を与える。また、公開鍵レジスタ403、秘密鍵レジスタ404は共に書き込み読み出し可能なレジスタとして構成している。

【0050】図5は、図4(a)における秘密鍵と公開鍵の更新の手順を示したものである。以下、ステップ51、52について説明する。なお、CKEとCKDは各々、共通鍵暗号処理部111で行う共通鍵暗号方式による暗号化と復号化を表わす。

【0051】STEP 51：公開鍵秘密鍵更新装置 501 は、特定コードを共通鍵暗号方式により第 1 の共通鍵生成値を鍵として暗号化してデータ RW0 を生成する。また、公開鍵 C を共通鍵暗号方式により第 1 の共通鍵生成値を鍵として暗号化してデータ RW1 を生成する。そして、データ RW0 と RW1 を送信側 IC カード 500 に転送する。

【0052】STEP 52：送信側 IC カード 500 は、データ RW0 を共通鍵暗号方式により第 1 の共通鍵生成値を鍵として復号化してデータ RW2 を生成する。そうして RW2 と特定コードを比較して両者が一致すれば認証は成立し、一致しなければ認証エラーとする。一致した場合は、データ RW1 を共通鍵暗号方式により第 1 の共通鍵生成値を鍵として復号化して公開鍵 C を生成し、公開鍵 A を公開鍵 C に更新する。さらに公開鍵 C と秘密鍵 A を入れ換える。以上のようにして公開鍵と秘密鍵の更新が行われる。

【0053】以上の構成により、定められた期間において公開鍵と秘密鍵が更新されるので、それらが公知となっても再び秘密にすることが可能であり、それら公開鍵、秘密鍵を用いることにより、IC カードおよび IC カードシステムの機密性を高めることが可能となる。

【0054】

【発明の効果】以上の構成により、本発明によれば、次の 1、2 の特徴によって暗号に用いる共通鍵、公開鍵、秘密鍵の機密性が高まるので、それらの鍵を用いた送受信装置および送受信方法において、送受信の機密性を高めることが可能となる。

【0055】1. 共通鍵や公開鍵や秘密鍵が公知になる可能性が低くなる。共通鍵は送受信装置の内部で生成され、また、相手側送受信装置に同じ共通鍵を所有させるために、共通鍵そのものを転送するのではなく、共通鍵を生成させるための情報を転送し、相手側送受信装置内部でも同様に共通鍵を生成させるため、送受信装置の内部構造がわからなくては共通鍵は導けないので、共通鍵が公知になる可能性は低くなる。

【0056】また、送受信装置の公開鍵をこの共通鍵を鍵として暗号化されて転送するので、公開鍵が公知になる可能性が低くなる。公開鍵が公知になる可能性が低くなるので、暗号化復号化関係にある秘密鍵が公知になる可能性も低くなる。

【0057】2. 共通鍵や公開鍵や秘密鍵が公知になっても、それらの鍵は更新される。共通鍵が公知になっても、共通鍵は相互認証における最初の認証までまたは毎回、鍵として用いられる度に更新されるので、公知となった共通鍵を用いて次の共通鍵暗号方式の暗号化復号化を行うことはできない。更に、送受信装置は共通鍵の履歴を格納するメモリを有しており、その履歴の期間内は異なった値の共通鍵を使うようにするために、公知になった共通鍵をすぐに繰り返し使ってしまうことがなく、それによってさらに機密性は高くなる。さらに、公開鍵および秘密鍵も必要に応じて更新することが可能である。

【図面の簡単な説明】

【図 1】本発明の一実施の形態に係わる IC カードのブロック図

【図 2】本発明の一実施の形態に係わる IC カードの共通鍵生成部のブロック図

【図 3】本発明の一実施の形態に係わるプロトコル図

【図 4】（a）公開鍵秘密鍵の更新をするための接続を示す図（b）本発明の一実施の形態に係わる、公開鍵と秘密鍵が更新可能な IC カードのブロック図

【図 5】公開鍵と秘密鍵を更新するためのプロトコル図

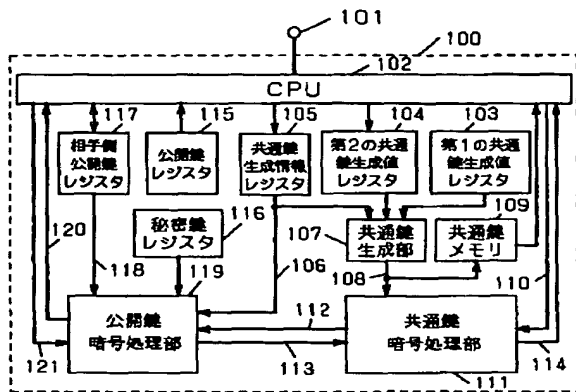
【図 6】従来の IC カードのブロック図

【図 7】従来の IC カードのプロトコル図

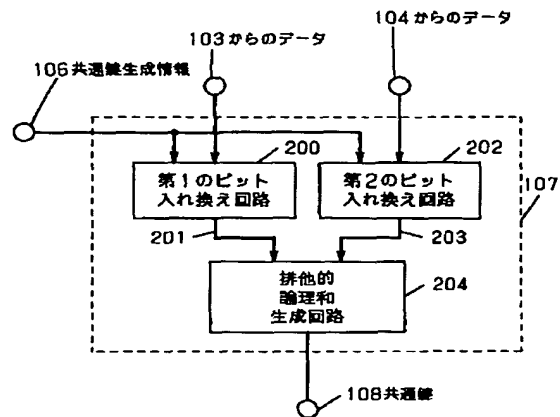
【符号の説明】

- 100 IC カード本体
- 101 入出力端子
- 102 CPU
- 103 第 1 の共通鍵生成値レジスタ
- 104 第 2 の共通鍵生成値レジスタ
- 105 共通鍵生成情報レジスタ
- 106 共通鍵生成情報
- 107 共通鍵生成部
- 108 共通鍵
- 109 共通鍵メモリ
- 111 共通鍵暗号処理部
- 115 公開鍵レジスタ
- 116 秘密鍵レジスタ
- 117 相手側公開鍵レジスタ
- 119 公開鍵暗号処理部
- 402 特定コード

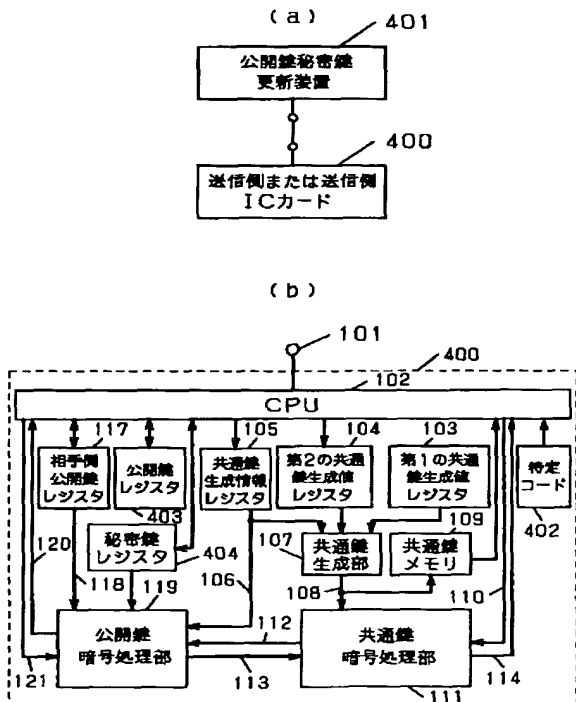
【図 1】



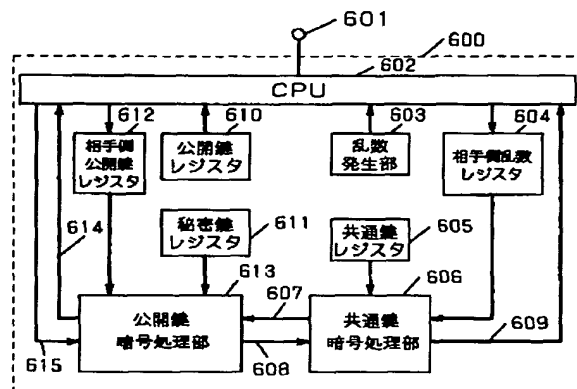
【図 2】



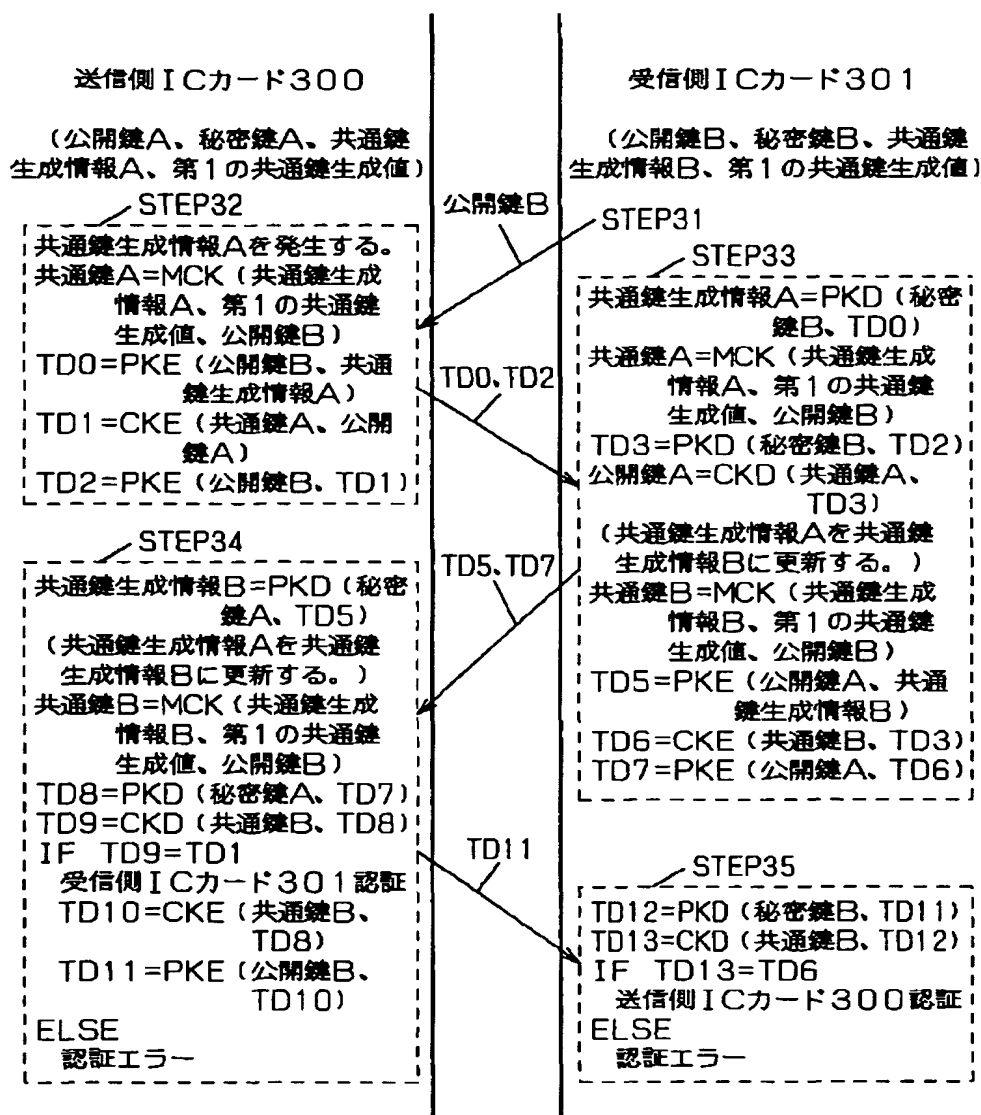
【図 4】



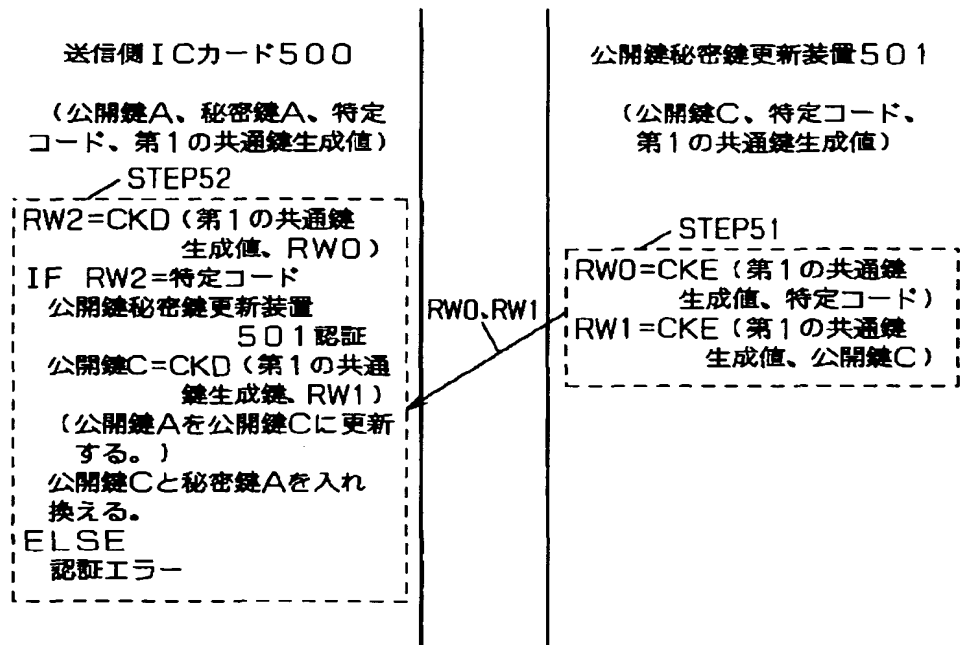
【図 6】



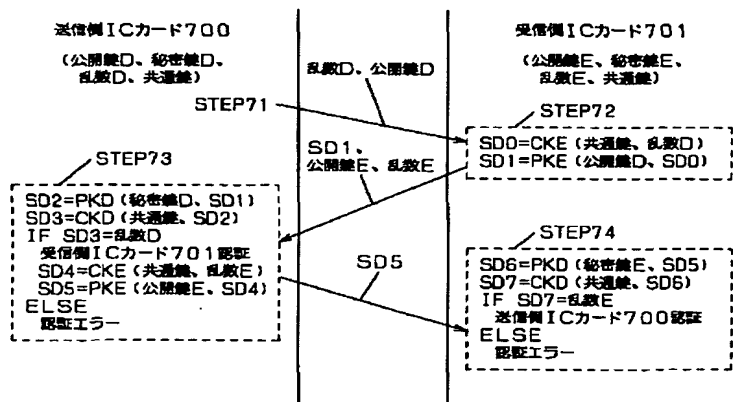
【図 3】



【図 5】



【図 7】



フロントページの続き

|                            |       |               |         |
|----------------------------|-------|---------------|---------|
| (51) Int. Cl. <sup>6</sup> | 識別記号  | F I           |         |
| G 0 6 K 19/10              |       | G 0 6 F 15/30 | 3 4 0   |
| G 0 9 C 1/00               | 6 6 0 | G 0 6 K 19/00 | R       |
|                            |       | H 0 4 L 9/00  | 6 0 1 E |